REMARKS

This application has been carefully reviewed in view of the above-referenced Office Action in which new grounds for rejection have been presented. Reconsideration is requested in view of the following remarks.

Regarding the cited art in general

The Maillard reference of record describes a conditional access system that uses smart cards at the receiver for decryption functions. As is apparently acknowledged by the Examiner, Maillard does not disclose encrypting certain content using a default key in the event of a communication failure (see paragraph spanning pages 3 and 4). The Office seems to assert that Maillard discloses a default encryption mechanism, but the undersigned is unable to find any such disclosure.

The Bestler reference of record, as understood, describes use of session data packets that are alternately encrypted/decrypted with two different session keys (col.3, lines 1-6). When a new key (a third key) is provided by the headend, one of the old keys continues to work for a time, while the other is rendered obsolete. New keys can thereby be introduced periodically as desired to enhance the system's security (col. 5, lines 19-22). Unauthorized users having only the obsolete key cannot decrypt the content once a polling cycle and key distribution cycle is complete (col. 5, lines 36-59). Although the current encryption key will continue to function when a polling cycle is missed (col. 5, lines 1-6), there is no disclosure for the continuation of encryption activity should a power fault or other system reset function occur and polling activity cannot be restarted due to a loss of communication with the content provider. A default key is discussed with reference to U.S. Patent no. 4,771,458. Reference to this patent indicates that the default key is used only for decryption of global data, not for addressed data "One of the global decryption keys is a permanent default key associated with the subscriber terminal to assure that communication with that terminal is possible despite a lack of knowledge of the terminal address or the other global decryption keys in its memory." (abstract) Thus, essentially, the default key is a key of last resort for communication of data between the headend and the subscriber

terminal. There is no teaching or suggestion of use of this default key for communication of A/V content.

Regarding the Rejections under 35 U.S.C. §103

Claims 1-57 are rejected as being unpatentable over Maillard et al. (US Patent No. 6,466,671, hereinafter "Maillard") in view of Bestler et al. (US Patent No. 4,995,080, hereinafter "Bestler").

Regarding claims 1, 9, 16, 23, 29 and 35, these claims have been amended to provide clarification. Claim 1 recites at least "encrypt certain audio/video content upon a communication failure between the conditional access encryption system and the conditional access management system in which said communication failure results in the termination of current encryption activity", claim 9 recites at least "encrypt certain audio/video content upon a communication failure between the conditional access system and the managing means in which said communication failure results in the termination of current encryption activity", claims 16 and 29 recite at least "a communication failure occurs between the conditional access management system and the conditional access system in which said communication failure results in the termination of current encryption activity", and claims 23 and 35 recite at least "communication cannot be established between the conditional access management system and the conditional access system such that said not establishing communication results in the termination of current encryption activity." In order to establish *prima facie* obviousness, the Office Action must establish the presence of each claim feature of in the cited art and provide articulated reasoning with rational underpinning for the obviousness of the combination of claim features and their interrelationship. The Office Action admits that Maillard does not specifically disclose the encryption of certain content upon a communication failure between the conditional access system and the conditional access management system and looks to Bestler to remedy this lack. The Office Action seems to assert that these claim features are met by Bestler at col. 3, lines 1-6, col 5, lines 19-22, col. 5, lines 37-39 and col. 5, lines 60-63, however, they are not.

Bestler in the recited sections, discloses at most a failure of communication due to a polling error of some type that restricts the subscriber from receiving the latest update for the

encryption for received content (col. 5, lines 1-6). There is no disclosure in Bestler for the special condition of what happens when a system reset of some type occurs in which the active encryption is lost due to the reset function, and polling cannot be re-established due to the loss of communication between the subscriber station and the provider. This is the condition that the claims as amended recite. Both Maillard and Bestler are silent with regard to any functioning, other than display of received content in the clear, when the encryption has been removed by a reboot (such as a power failure) and communication between subscriber and provider cannot be re-established to restart polling. The recited claims provide for a solution in this instance by providing for a default encryption to be recalled from a local storage memory location and placed into use by the encryption process of the subscriber station such that all received content may continue to be decrypted and displayed properly until communication can be re-established. The combination of Maillard and Bestler do not provide the disclosure necessary to render the claims, as presented, obvious. Reconsideration and allowance of claims 1, 9, 16, 23, 29, and 35 is hereby respectfully requested.

Regarding independent claims 41, 47, and 52, these claims each recite calls for a similar feature of "audio/video content normally being decrypted using an even decryption engine and an odd decryption engine operating by use of alternate decryption keys" and "use of the default decryption information when a communication failure at an audio/video content provider would otherwise permit content to be provided without benefit of encryption for decryption using the alternate decryption keys by the odd and even decryption engines". The Office Action admits that Maillard does not disclose at least an even and an odd decryption engine for use in decrypting content. The Office Action looks to Bestler to remedy this lack, citing col. 5, lines 32-35, however, it does not. In addition, this is not the only recited claim element lacking in the combination of Maillard and Bestler. There is no disclosure in either Maillard or Bestler for the recited claim feature of "use of the default decryption information" when there is a communication failure that would otherwise permit content to be provided without the benefit of encryption, and there is no disclosure in Bestler for an odd and even decryption engine.

Bestler, in the sections recited, discloses multiple encryption keys that are sent by a provider to a subscriber, and a process for continuing to decrypt provided content within the

subscriber station by providing two different decryption keys that both will decrypt received content, then sending another key that will decrypt content while simultaneously disabling one of the two earlier keys. This is an efficient means for delivering additional decryption keys such that content continues to be decrypted by the most updated keys. However, this does not address the condition that the recited claim elements address. In the claims as presented, content is decrypted by two alternate keys, one used in an odd decryption engine and one in an even decryption engine. Thus, portions of content may be decrypted by each decryption engine, but if one key is invalid the subscriber may decrypt only a portion of the received content. This is very different than the disclosure in Bestler. In addition, if all communication is lost, such as that which may occur because of a power outage reboot, the claims recite a feature whereby the system may continue to receive and decrypt content without benefit of instruction from the provider until communication with the provider can be re-established. The disclosure in Bestler assumes constant communication with the provider such that new keys may always be provided for replacement of outdated or obsolete decryption keys. This is not the same as the recited features in claims 41, 47 and 52 as amended. Therefore, the combination of Maillard and Bestler does not provide the disclosure to render claims 41, 47, and 52 obvious. Reconsideration and allowance of claims 41, 47 and 52 is hereby respectfully requested.

Regarding claims 2-8, 10-15, 17-22, 24-28, 30-34, 36-40, 42-46, 48-51 and 53-57, these claims are rejected over the combination of Maillard and Bestler. However, claims -8, 10-15, 17-22, 24-28, 30-34, 36-40, 42-46, 48-51 and 53-57 each depend from one of claims 1, 9, 16, 23, 29, 35, 41, 47 and 52. As such, the applicants submit that these claims are patentable over the combination of Maillard and Bestler for at least the reasons stated above. Accordingly, reconsideration and allowance are respectfully requested.

Concluding Remarks

The undersigned additionally notes that many other distinctions exist between the cited art and the claims. However, in view of the clear distinctions pointed out above, it is submitted that further discussion is unnecessary. No amendment made herein was related to the statutory

requirements of patentability unless expressly stated herein. No amendment made was for the purpose of narrowing the scope of any claim unless an argument has been made herein that such amendment has been made to distinguish over a particular reference or combination of references.

Interview Request

In view of this communication, all claims are now believed to be in condition for allowance and such is respectfully requested at an early date. If further matters remain to be resolved, the undersigned respectfully requests the courtesy of an interview. The undersigned can be reached at the telephone number below.

Respectfully submitted,

/Jerry A. Miller 30779/

Jerry A. Miller
Registration No. 30,779

Dated: August 25, 2008

Please Send Correspondence to:
Miller Patent Services
2500 Dockery Lane
Raleigh, NC 27606
Phone: (919) 816-9981
Fax: (919) 816-9982
Customer Number 24337